

Student

Professor

Course

Institution

Date

Table of Contents

Table of Contents	Page 2
Introduction	Page 3
Functionality of Social Media Websites	Page 4
Usage Patterns of Social Networking Websites	Page 5
Privacy and Demographics	Page 6
Privacy Issues about Social Networking Websites	Page 9
Trust within Social Networking Communities	Page 12
Conclusion	Page 13
References	Page 14
Appendix I	Page 15
Appendix II	Page 16
Appendix III	Page 17

Introduction

Over the last few decades the development of social networks on the Internet has become increasingly popular and several prominent websites have been created where users can meet their friends in a virtual world such as Facebook, Twitter and MySpace. These social networking websites have several benefits which allow users to host profiles and to share information with their friends, family and even strangers. However, social networks also have several concerns for users about issues such as privacy, identity theft and invasive advertising. Indeed, Agosto and Abbas comment that "in today's highly networked world, more personal information is available to more people than ever before, and questions of personal privacy and information security must be considered" (Agosto & Abbas, 2011, p. 60). Furthermore, the creation of modern social networks has caused significant privacy issues which are becoming increasingly prevalent for the stakeholders in this contentious issue, especially as more people join social networks and malicious users attempt to get access to their personal information for nefarious purposes.

The concept of online social networking has evolved from a small phenomenon to a widely accepted part of popular global culture. Communication across the Internet has emerged over the last few decades as this technology has grown. However, in addition over the last decade, the Internet has seen a rapid increase in the development of social networks. This significant increase in user participation in social networking has also been influenced by the diversification and technical sophistication that these various websites can offer. Indeed the development of online social networks has seen several prominent websites covering different categories including business-based social networks, blogging, dating or friendship websites, as well as other types of social media websites.

Functionality of Social Media Websites

While these several different categories have influenced the development of social networks in various areas the boundaries between these types of social networking websites are not clear. However, the core functionality behind the most prominent social networking sites gives the users a chance to create a profile which represents their online presence. The main purpose of creating a profile, regardless of the type of social networking site, is for other users to be able to search and contact a person based on their profile information. Indeed, Agosto and Abbas also assert that "online social networking is an extension of social communication in the offline world, in which the sharing of personal information is crucial for building and maintaining peer relationships" (Agosto & Abbas, 2011, p. 61). Over the last decade, websites have emerged such as Friendster which is used to find friends, sites such as LinkedIn which can be used to find new jobs or Facebook which helps users develop an online social network between their friends and colleagues as well as other users of the website. All these social networking websites have experienced periods of rapid growth and at the start of the 21st century websites such as Facebook and Twitter have hundreds of millions of concurrent users. The concept behind social networking websites means that users have to give their personal information to the website operators while the creation of a user profile can lead to privacy implications for all stakeholders, especially if the website's default security settings are not applied.

Usage Patterns of Social Networking Websites

While the various social networking sites that are available online share a similar concept of creating and developing interpersonal interaction and communication between users, the specific aims of the website's usage pattern vary across the different platforms. The most important concept behind a social networking site is based on the creation and promotion of the user's profile as well as a visualization of the user's network relations. Furthermore, content can be posted to other user profiles which can be seen by both users and nonusers of the various social network sites which are available. In the case of websites such as Friendster and Facebook this model has formed the fundamental basis for the way the website operates. However, in dating websites, the creation of a profile is one of the most important aspects of the site while the visualization of the uses network is kept private.

Therefore, it seems that the patterns of usage for the various social networking sites are different while the information that can be disclosed on various websites is also variable. Indeed, the concept of identity is treated differently across the various kinds of social network sites. In the case of the business-based social network, LinkedIn, the website encourages the use of real names by the website's users. However, in the case of websites such as Match.com which offers casual dating services, the users are able to create an element of anonymity by using a unique username and not the user's real name. Furthermore, the personal information revealed by users can also be different based on the type of website the user registers with. Indeed in the case of Facebook, the user's profile includes information about personal interests, hobbies, favorite movies, music the user enjoys and other personal data.

However, on dating sites this information is not as important because users want to keep up some anonymity on the website while on social networking sites which are based on adult content the disclosure of private user information such as sexual preference is encouraged. This presents a privacy issue especially because membership of dating sites has been on the increase over the recent years. Indeed, data from the Pew Research Center shown in Appendix III indicates that across all demographics, Americans are increasingly using such websites (Pew Research Center, 2016). In addition, the visibility of a user's profile information across the various social networking sites is also an issue for all stakeholders. On certain social network sites every user of the site may be able to see the profiles of all the members of the sites. However, on sites such as Facebook and LinkedIn which contain a large amount of personal information users are able to control the visibility of all the elements of the profiles. Indeed, the variety of social networking sites suggests that users are happy about disclosing information under certain circumstances while they are unhappy to show their personal information in a different situation.

Privacy and Demographics

The issue of privacy on social networking websites is also a demographic and geographical issue for stakeholders because of the global prevalence of the Internet and the ability of websites such as Facebook and Twitter to be available to people around the world regardless of where they live or their language. Indeed, Nissenbaum states that "the prodigious capacity of information technology and digital networks to publish and disseminate information has given rise to a host of privacy problems" (Nissenbaum, 2010, p. 216) at the start of the 21st century. In addition, the development of human society has seen the next generation of young people become less concerned about traditional social problems in addition to accepting that the

disclosure of information related to a person's privacy may occur from using social networking websites. The current generation has grown-up with the internet and the concept of social networking while they also feel comfortable with disclosing their personal information on the internet. This is in contrast to the older generation who do not embrace the use of modern technology and who are still wary of disclosing their personal information and wary of traditional privacy issues such as identity theft or fraud. However, according to data from the Pew Research Center as shown in Appendix II regardless of demographics, a large percentage of the American population believes their personal information is not completely secure (Pew Research Center, 2015).

The generational issue over the problem of online privacy is clear through the way young people have embraced social networking and do not seem concerned about disclosing information about their personal privacy. Indeed, the young generation of online stakeholders seems to be publishing more personal information than ever while uploading a greater amount of content to the Internet. Statistics from the Pew Research Center support this theory especially because a 2012 survey revealed that teens were revealing more personal information than ever as illustrated in Appendix I (Pew Research Center, 2013). This argument is supported by Sarat et al who assert that "traditionally people worried about public invasions of the private domain, but social networking sites now invite disclosure of information that previously would have been regarded as private" (Sarat, Douglas, & Umphrey, 2012, p. 8). The ability of young people to create social networking profiles could have long-term repercussions as governments and employers are able to search for a person's comments on social media. As well as the difference in the way people from different generations use technology, social networking sites can also use social engineering to find out more user information by using algorithms which can create

privacy issues for the users and other stakeholders. The use of third-party databases which collate publicly available information about a website's user base are also important because these third-party organizations can buy user data from unscrupulous companies willing to compromise their users and their personal information for a profit. This technique of manipulating user information has serious privacy issues if social networking website owners use this private information for advertising or malicious purposes.

Furthermore, when users choose to share personal information over a certain social network it is not initially obvious which Internet users can view the profile. The question of whether the profile can only be seen by users who are registered with the website or whether external users have access to private information is becoming increasingly important as more social networks appear online. User privacy could also be compromised by social networks which use third-party applications such as games, multimedia sharing or video streaming to compile information, especially if this information is accessible by a third-party application developer who can then sell this information on to another party. The users of social networking sites are all sharing some of their personal information to a certain extent. However, when a website is acquired by another company than the user's information can be interpreted or used in an unauthorized way. Therefore, social networks have created significant privacy issues for their stakeholders over the last few decades because users are able to share their personal information with the rest of the Internet. Indeed users can expose themselves to several risks by sharing information such as their name, date of birth, address or other information such as pictures which could be used for identity theft or other criminal activities.

It has become clear that social networking websites share a similar purpose which is promoting online interaction and interpersonal communication between the users of such a

website. However, the aims and patterns of usage across the various services which are available on social networking websites are very different. The fundamental concept behind social networking websites is based on the creation of the user's profile and the presentation of this information along with a network of friends or family to the entire user base of the website. This concept lies behind most social networking sites regardless of the type of website which work through the flow of information between the site's users. A website such as Match.com which offers dating services uses profiles as the most important part of the website however there is no visualization of the user's friend network. In social networking sites such as blogger.com the user's profile is a secondary part of the website compared with the content that is uploaded. Therefore, social networking websites have a multitude of uses, especially the way users share their personal information across these networks which can also be very different and depends on the purpose of the site. Indeed, on sites such as Facebook or LinkedIn it is important to create an online profile which represents the user's real-life identity. However, on websites such as Friendster the user is not forced to use their real name creating anonymity between the user and their online profile.

Privacy Issues about Social Networking Websites

Another feature of social networking sites which could have serious privacy issues for stakeholders is the publication of personal photos. A user's personal information could be revealed through the content of certain pictures especially about the user's personal interests or hobbies. However, personal information such as current employer, education background, or personal information such as drug use or sexual preferences could also be revealed by publishing personal photos. The publication of such material on social networking sites is constantly changing and on certain sites there are no privacy settings on a user's profile. However, social

networking sites such as Facebook and LinkedIn have options to restrict whether users or nonusers are able to get access to a profile. The cost of a user's privacy is also an important issue in the context of the impact on the stakeholders of social networking websites especially because of the lack of global legislation to control how the various social networking websites handle and store their user's personal information. Some social networks in developing countries violate the basic human rights which are designed to protect their personal information. For example, in authoritarian countries such as Iran the use of western social networking sites is illegal however locally produced social networking sites are forced by the government to show the user's information on their profile. Furthermore, this particular social network has several features to find out who has looked at a user's profile while it is also possible for users to buy information about who has viewed their profile. This situation has arisen and is dangerous for stakeholders in social networking because of the lack of comprehensive global legislation to control how websites use personal information.

An examination of social networking websites must also be conducted with regards to network theory which illustrates that the relationship between a person's privacy and their social network is multidimensional. On certain social networking sites such as LinkedIn or Facebook users want their personal information to be restricted and only available to their close friends. However, on social networking sites such as dating sites the users are happy for some aspects of their personal information to be revealed to strangers but not to close friends, especially if the social networking site is related to dating. Indeed, network theory can be applied to online social networking websites to illustrate how a person's social network can contain several relationships of different strengths and depths. The use of this particular theory in the study of personal information and how it is revealed online demonstrates the existence of several differences

between a user's online and off-line situations. A user's off-line social network is composed of relationships that can be defined as either weak or strong while these relationships are often diverse, especially in relation to how intimate the user perceives their relations with others to be. However, online social networks usually cut out the individual nuances of personal relationships to a simple condition of either being a friend or not. Indeed, there is no way of measuring the context of the relationship between two people in an online environment where the relationship is a binary choice of either being a friend or not.

The definition of being a friend also varies across several social networks as some users are happy to accept any other of the site's users as a friend. However, other users stick with the traditional off-line definition of a friend and only accept people on their online profile if they are friends in real-life. Therefore, in some instances the users of social networks can have several friends online that are not actually their friends in the real world. This can also have serious privacy implications because a user's behavior towards their online friends can lead to personal information being inadvertently revealed. In addition, while a user's off-line network may only include dozens of connections their online network may list several dozen or hundreds of connections. The implication of this for stakeholders is that a user's online social networks are larger than a user's off-line network however it seems that the ties between each node of the user's network are much stronger in the off-line model. Indeed, online social networks promote the creation of weaker ties between users which can have significant effects about the privacy of the user's personal information. In the case of a user with hundreds of weak connections on their online social network their personal information is widely available while the threshold to become a friend of this particular the user is also very low posing a significant threat to that user's information privacy.

Trust within Social Networking Communities

It seems that the trust within a community of users on online social networks must be very different to the trust in their off-line network. Indeed, in the online environment users are happy to give their personal information to a large audience linked to the user by a relatively weak connection. Therefore, while the issue of privacy must be determined as necessary and conducive for the creation of an intimate offline relationship, the trust between users decreases within the online model of a social network. In addition, the creation of a new kind of intimacy between online users is becoming increasingly prevalent as people share their personal information with increasingly larger and unknown groups of people. Furthermore, there are several privacy implications for stakeholders as a result of the development of social networks over the last decade. It seems that the users of online social networks such as Facebook, Twitter, LinkedIn and various other dating or blogging sites are relatively unconcerned about sharing their personal information online. Indeed, on all social networking sites personal data is needed to create a public profile while in general, the users of social networking sites do not tend to limit the availability or privacy of their information. In the case of websites such as Facebook, as a consequence of the variety of personal information which is required or disclosed in the users profile, significant privacy options for all users have been created by the website. However, in the case of users who are oblivious or unconcerned about the disclosure of their personal information, the use of social networks can put users in danger from malicious attackers who want to get access to the user's personal information.

The operators of social networking websites have to be able to make it easier for their users to carry out specific privacy controls on their personal information so that even in the case of a new user they can clearly control what information other users can see from the start. Social

networking websites must use strong default settings to prevent information from being published without the user's explicit knowledge. Therefore, in the future, the user must be able to make the choice about what information to publish and what information the public or members of the user's network can see. Furthermore, to protect stakeholders, all social networking websites should be forced to display warnings to help their users decide which aspects of their profile are available. In addition, social networking websites must create challenge/response systems to prevent the automated harvesting of user information by bots which can also cause privacy issues for stakeholders.

Conclusion

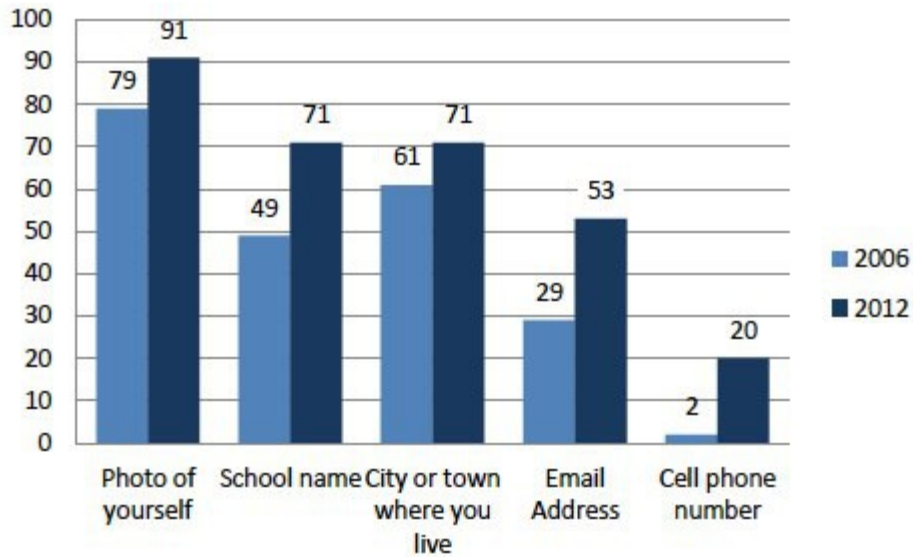
Therefore, in conclusion social networks have emerged over the last decade and have enabled people to develop large online networks. The new generation of Internet users may have hundreds of connections in their social networking profile however not all these connections could be considered as a person's off-line friend. Indeed, privacy issues have surfaced recently because most connections on a user's network are strangers which have access to the user's personal information. As a result of the information that users willingly give to social networking sites to complete their profile, these users unnecessarily expose themselves to several different privacy risks which are not unique to one social network but are common to them all. When making a profile on a social networking website, users should be careful not to reveal too much information about their identity as well as protecting their own rights through the use of privacy settings which offers the user complete control over their ability to protect their private information.

References

- Agosto, D. E., & Abbas, J. (Eds.). (2011). *Teens, Libraries, and Social Networking: What Librarians Need to Know* (Libraries Unlimited Professional Guides for Young Adult Librarians). Santa Barbara, CA: Libraries Unlimited.
- Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press.
- Pew Research Center. (2013, May 21). *Teens, Social Media and Privacy*. Retrieved from Pew Research Center: <http://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/>
- Pew Research Center. (2015, May 20). *Americans' Attitudes About Privacy, Security and Surveillance*. Retrieved from Pew Research Center: <http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>
- Pew Research Center. (2016, February 11). *15% of Americans use online dating sites or mobile apps*. Retrieved from Pew Research Center: <http://www.pewinternet.org/2016/02/11/15-percent-of-american-adults-have-used-online-dating-sites-or-mobile-dating-apps/>
- Sarat, A., Douglas, L., & Umphrey, M. M. (Eds.). (2012). *Imagining New Legalities: Privacy and Its Possibilities in the 21st Century*. Stanford, CA: Stanford University Press.

Appendix I

Social media profiles: What teens post – 2006 vs. 2012

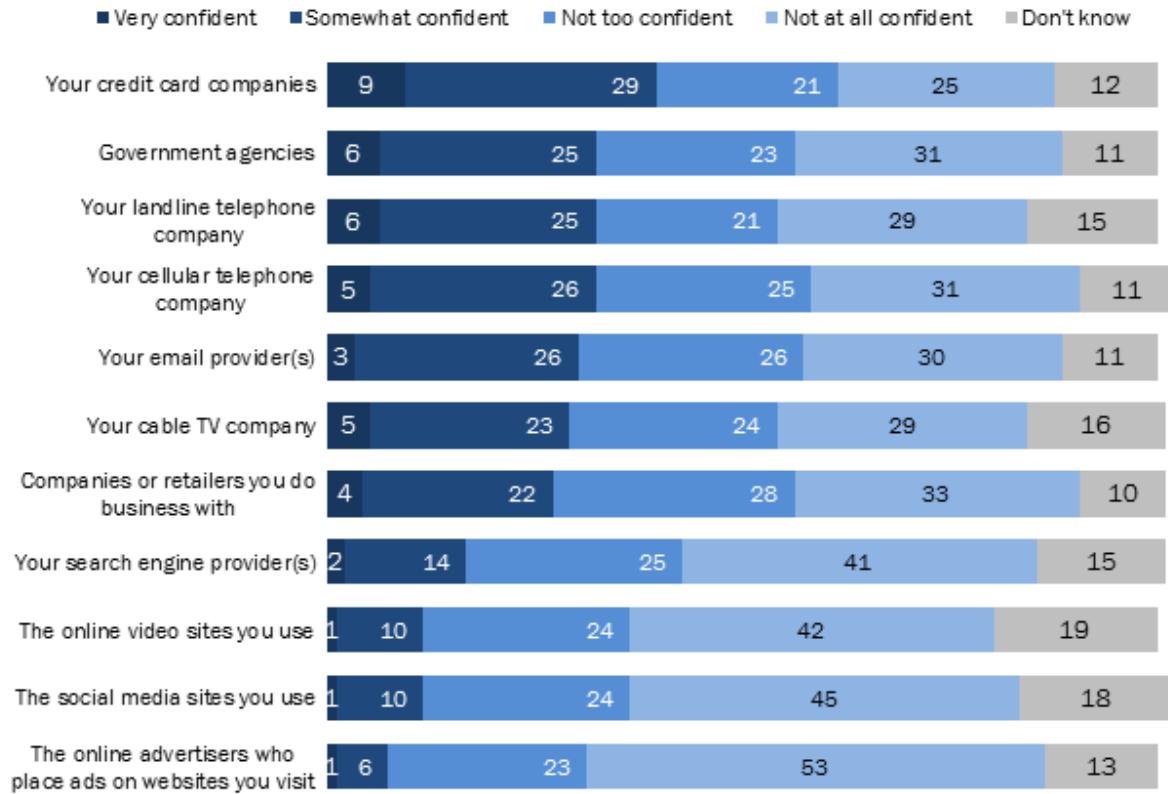


Source: Pew Internet Parent/Teen Privacy Survey, July 26-September 30, 2012. n=802 teens ages 12-17. Interviews were conducted in English and Spanish and on landline and cell phones. Margin of error for results based on teen social media users is +/- 5.1 percentage points. Comparison data for 2006 comes from the Pew Internet Parents & Teens Survey, October 23-November 19, 2006. n=487 teens with a profile online. Margin of error is +/- 5.2 percentage points.

Appendix II

Few Express Confidence That Their Records Will Remain Private and Secure

% of adults who say they are ... that the records of their activity maintained by various companies and organizations will remain private and secure



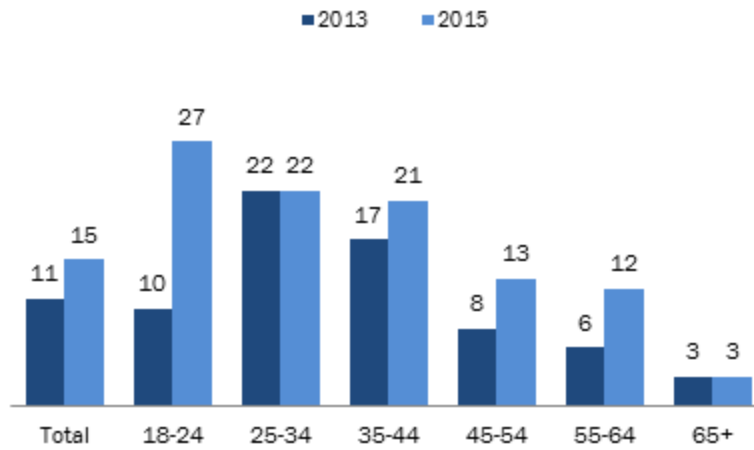
Source: Pew Research Center's PrivacyPanel Survey #2, Aug. 5, 2014-Sept. 2, 2014 (N=498). Refused responses not shown.

PEW RESEARCH CENTER

Appendix III

Use of online dating sites or mobile apps by young adults has nearly tripled since 2013

% in each age group who have ever used an online dating site and/or mobile dating app



Source: Survey conducted June 10-July 12, 2015.

PEW RESEARCH CENTER
